4.4 Congestion Control and Quality of Service

-compiled by UBM

Introduction

- *The main focus of congestion control and quality of service is data traffic.*
- *In congestion control we try to avoid traffic congestion.*
- *In quality of service, we try to create an appropriate environment for the traffic.*
- *So, before talking about congestion control and quality of service, we discuss the data traffic itself.*

Figure 24.1 *Traffic descriptors*

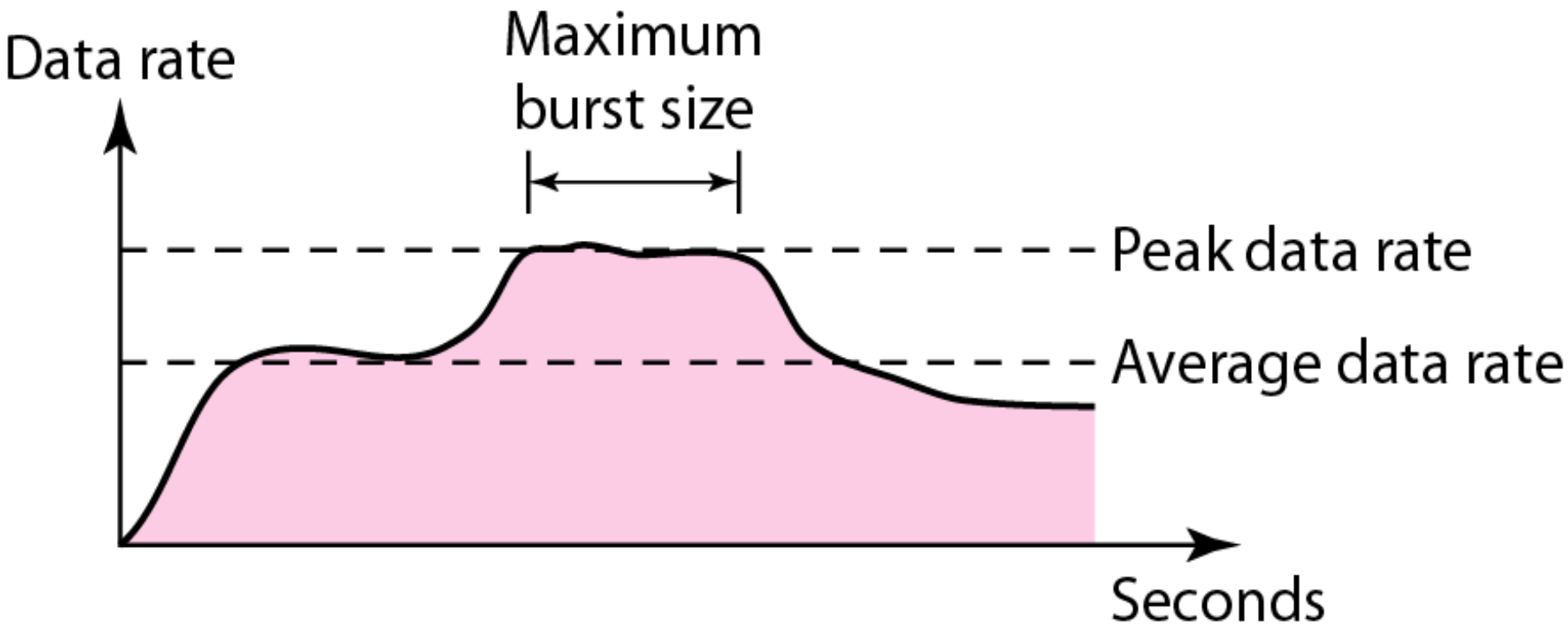
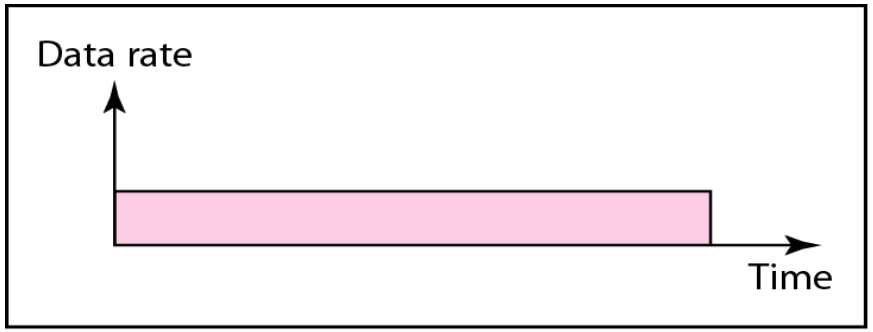
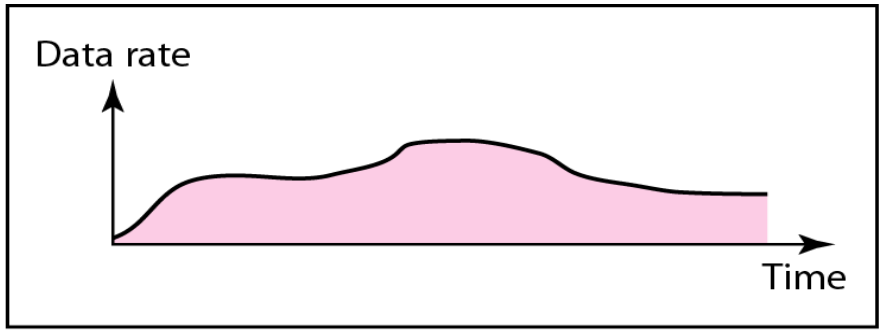


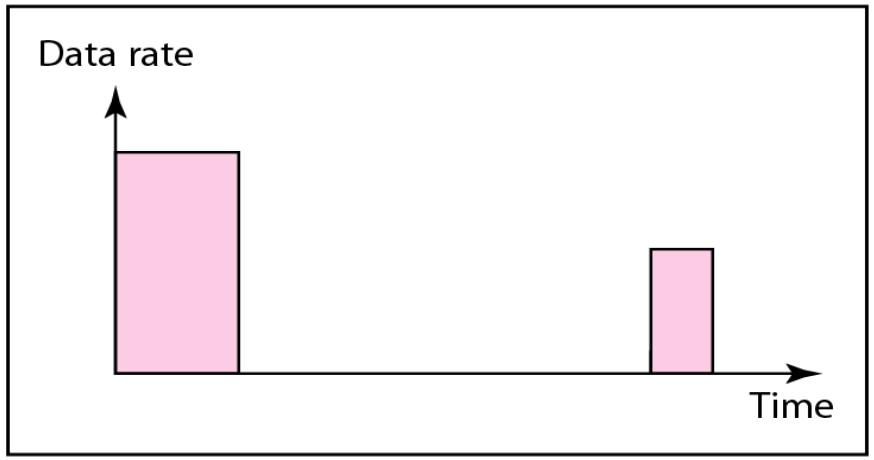
Figure 24.2 *Three traffic profiles*



a. Constant bit rate



b. Variable bit rate



c. Bursty

Congestion

- *Congestion in a network may occur if the load on the network—the number of packets sent to the network—is greater than the capacity of the network—the number of packets a network can handle.*
- *Congestion control refers to the mechanisms and techniques to control the congestion and keep the load below the capacity.*

Figure 24.3 *Queues in a router*

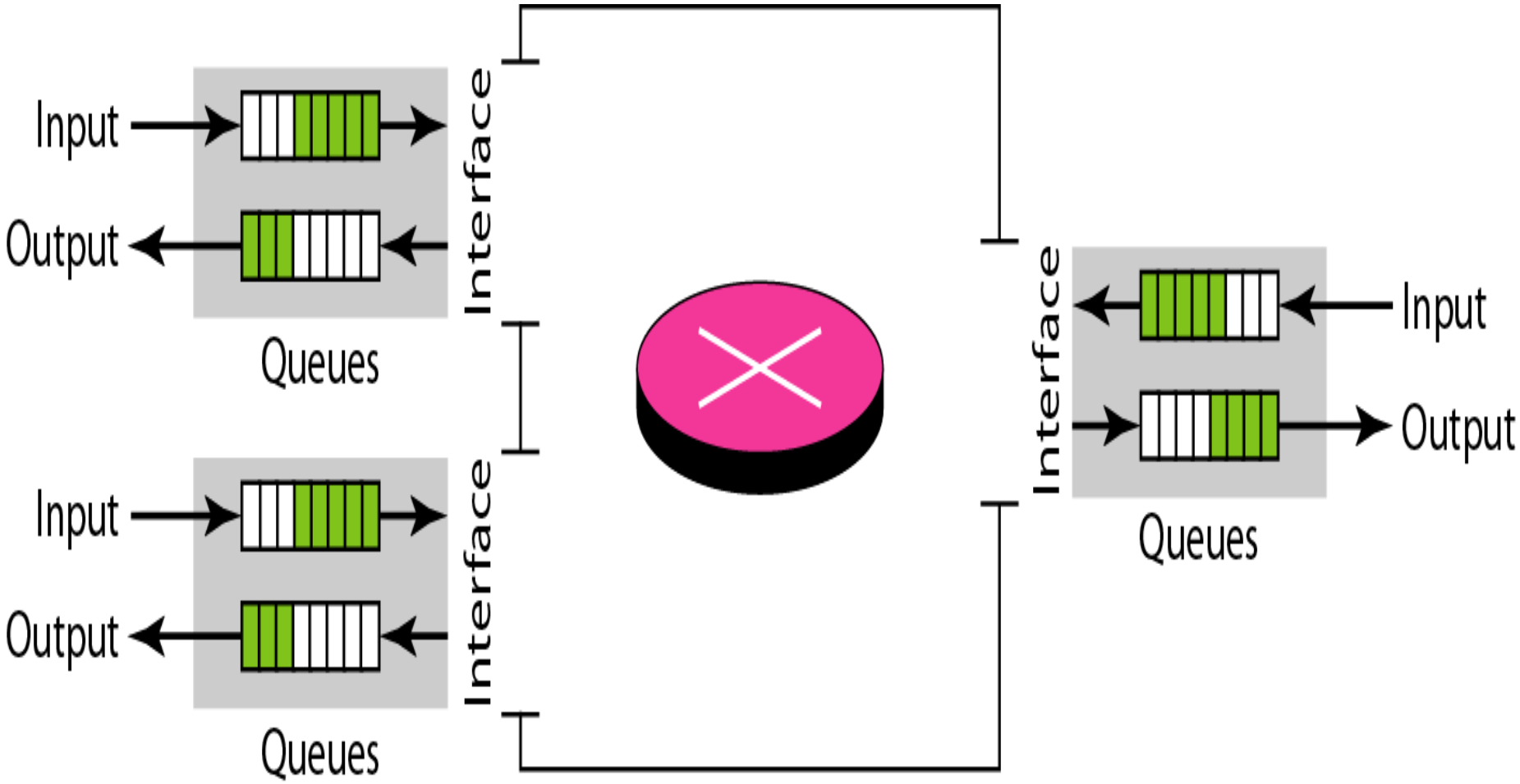
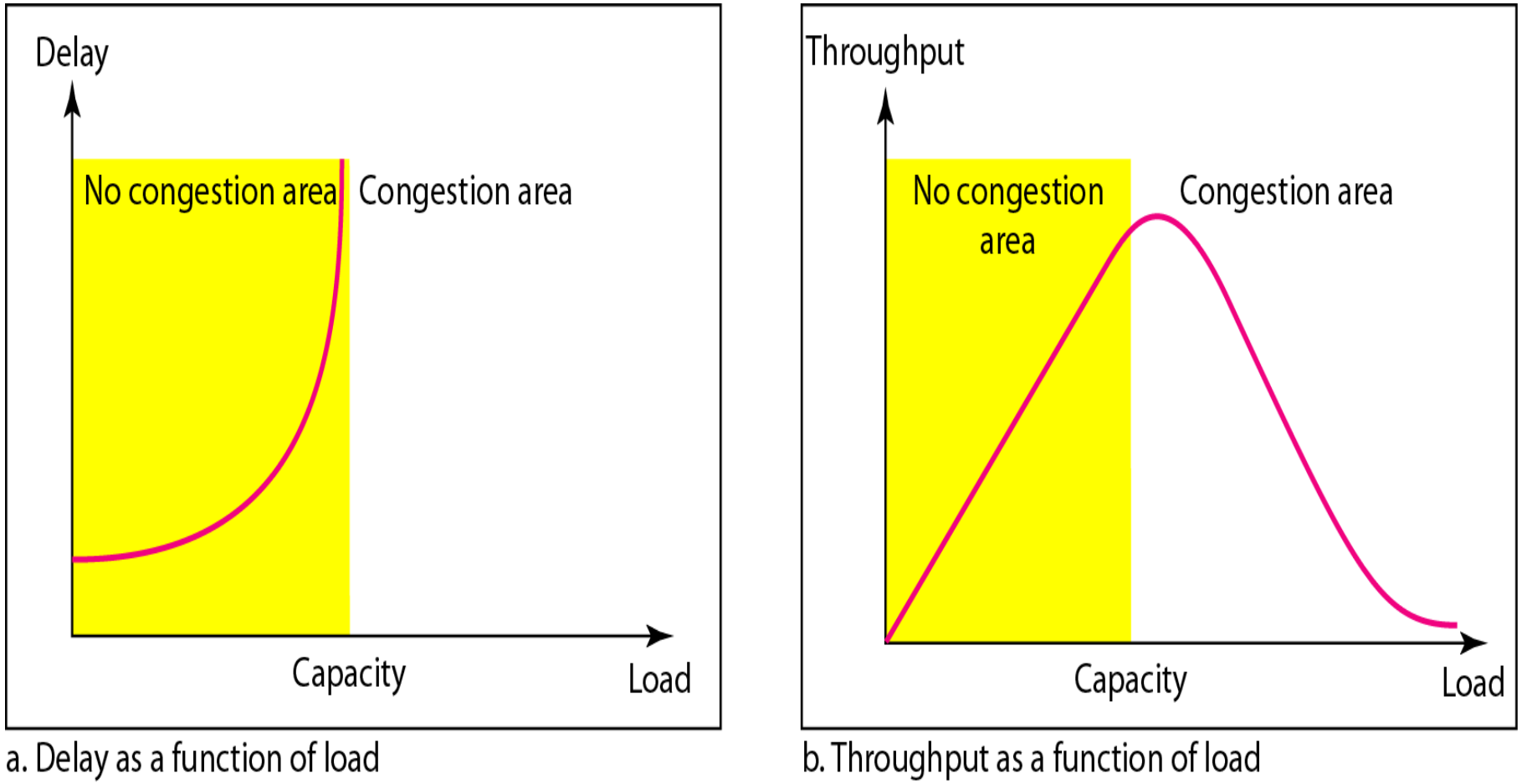


Figure *Packet delay and throughput as functions of load*



a. Delay as a function of load

b. Throughput as a function of load

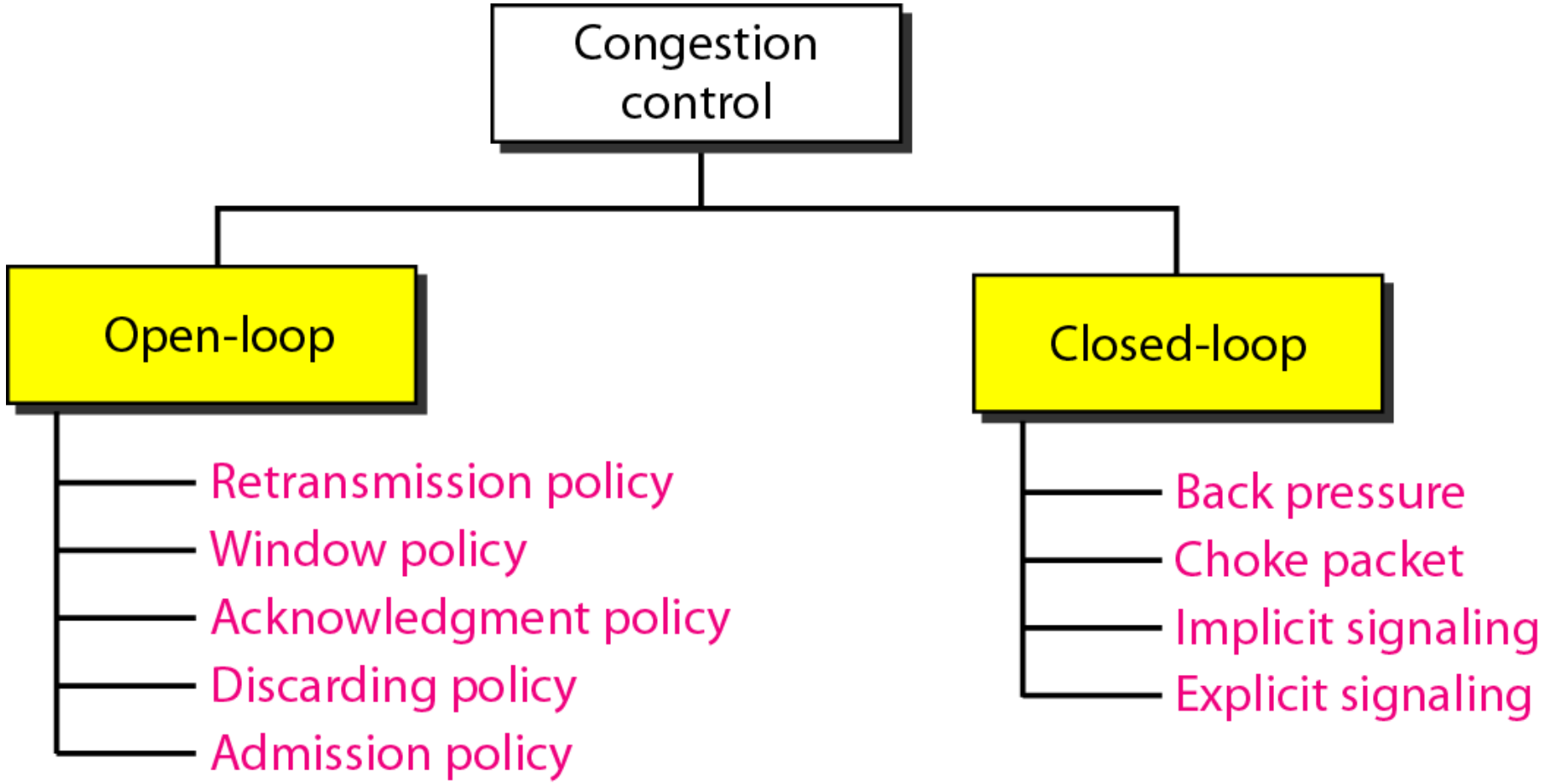
24-3 CONGESTION CONTROL

Congestion control refers to techniques and mechanisms that can either prevent congestion, before it happens, or remove congestion, after it has happened. In general, we can divide congestion control mechanisms into two broad categories: open-loop congestion control (prevention) and closed-loop congestion control (removal).

Topics discussed in this section:

Open-Loop Congestion Control
Closed-Loop Congestion Control

Figure 24.5 *Congestion control categories*



Open Loop Congestion Control Policies

- **Retransmission Policy :**
  It is the policy **in which retransmission of the packets are taken care.**
  If the sender feels that a sent packet is lost or corrupted, the packet needs to be retransmitted. This transmission may increase the congestion in the network.
  To **prevent congestion, retransmission timers must be designed to prevent congestion and also able to optimize efficiency.**

Open Loop Congestion Control Policies

- **Window Policy :**
  The type of window at the sender side may also affect the congestion. **Several packets in the Go-back-n window are resent, although some packets may be received successfully at the receiver side**. This duplication may increase the congestion in the network and making it worse.
  Therefore, **Selective repeat window should be adopted as it sends the specific packet that may have been lost.**

Open Loop Congestion Control Policies

- **Discarding Policy :**
  A good discarding policy adopted by the routers is that the routers **may prevent congestion and at the same time partially discards the corrupted or less sensitive package and also able to maintain the quality of a message.**
  In case of **audio file transmission, routers can discard less sensitive packets to prevent congestion** and also maintain the quality of the audio file.

Open Loop Congestion Control Policies

- **Acknowledgment Policy :**
  Since acknowledgement are also the part of the load in network, the acknowledgment policy imposed by the receiver may also affect congestion. Several approaches can be used to prevent congestion related to acknowledgment.
  The receiver should send acknowledgement for N packets rather than sending acknowledgement for a single packet. The receiver should send a acknowledgment only if it has to sent a packet or a timer expires.

Open Loop Congestion Control Policies

- **Admission Policy :**
  In admission policy a mechanism should be used to prevent congestion. **Switches in a flow should first check the resource requirement of a network flow before transmitting it further. If there is a chance of a congestion or there is a congestion in the network, router should deny establishing a virtual network connection to prevent further congestion**.

Open Loop Congestion Control Policies

- Open loop congestion control policies **are applied to prevent congestion before it happens.** The congestion control is handled either by the source or the destination.

Closed Loop Congestion Control

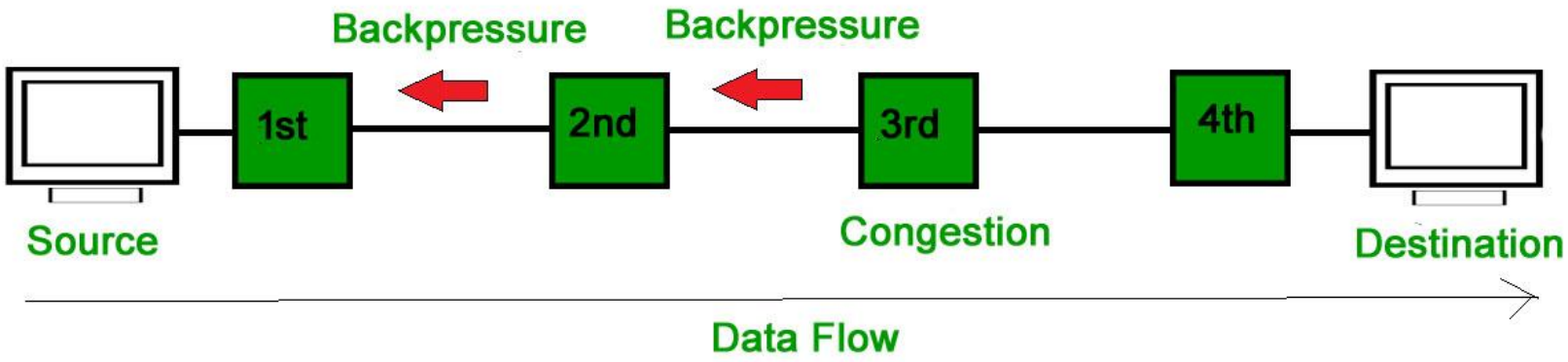
- **Closed loop congestion control technique is used to treat or alleviate congestion after it happens.** Several techniques are used by different protocols; some of them are:

Closed Loop Congestion Control

- **Backpressure :**
  Backpressure is a **technique in which a congested node stop receiving packet from upstream node.** This may cause the upstream node or nodes to become congested and rejects receiving data from above nodes. Backpressure is a node-to-node congestion control technique that propagate in the opposite direction of data flow. The backpressure technique can be **applied only to virtual circuit where each node has information of its above upstream node.**

Closed Loop Congestion Control

Backpressure :



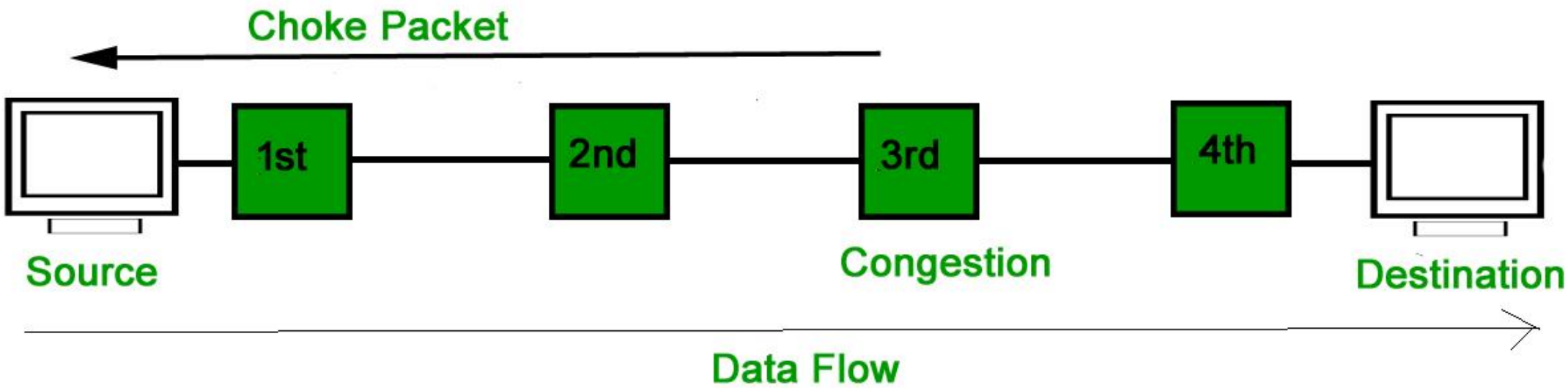
In above diagram the 3rd node is congested and stops receiving packets as a result 2nd node may be get congested due to slowing down of the output data flow. Similarly 1st node may get congested and informs the source to slow down.

Closed Loop Congestion Control

- **Choke Packet Technique :**
  Choke packet technique is applicable to both virtual networks as well as datagram subnets. **A choke packet is a packet sent by a node to the source to inform it of congestion**.
- **Each router monitor its resources and the utilization at each of its output lines. whenever the resource utilization exceeds the threshold value which is set by the administrator, the router directly sends a choke packet to the source giving it a feedback to reduce the traffic**.
- The intermediate nodes through which the packets has travelled are not warned about congestion.

Closed Loop Congestion Control

Choke Packet Technique :



Closed Loop Congestion Control

- **Implicit Signalling :**
  In implicit signalling, **there is no communication between the congested nodes and the source**.
- **The source guesses that there is congestion in a network.**
- For example **when sender sends several packets and there is no acknowledgment for a while**, one assumption is that there is a congestion.

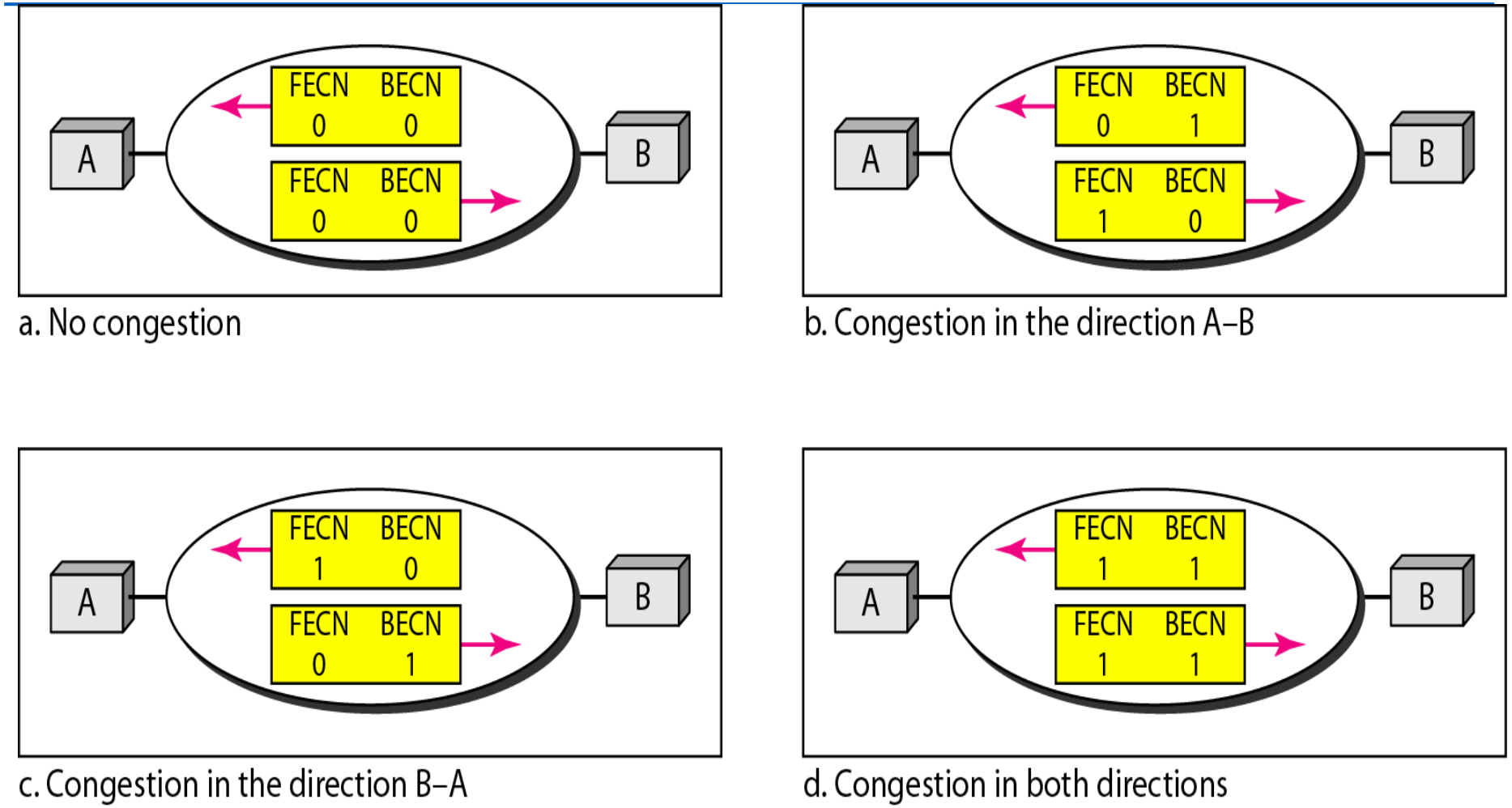
Closed Loop Congestion Control

- **Explicit Signalling :**
  In explicit signalling**, if a node experiences congestion it can explicitly sends a packet to the source or destination to inform about congestion.**
- The difference between **choke packet and explicit signalling is that the signal is included in the packets that carry data rather than creating different packet as in case of choke packet technique**.
  Explicit signalling can occur in either **forward or backward direction.**

Closed Loop Congestion Control

- **Forward Signalling :** In forward **signalling signal is sent in the direction of the congestion. The destination is warned about congestion.** The receiver in this case adopt policies to prevent further congestion.
- **Backward Signalling :** In **backward signalling signal is sent in the opposite direction of the congestion. The source is warned about congestion and it needs to slow down.**

Figure 24.14 *Four cases of congestion*



24-5 QUALITY OF SERVICE

Quality of service (QoS) is an internetworking issue that has been discussed more than defined. We can informally define quality of service as something a flow seeks to attain.

Topics discussed in this section:

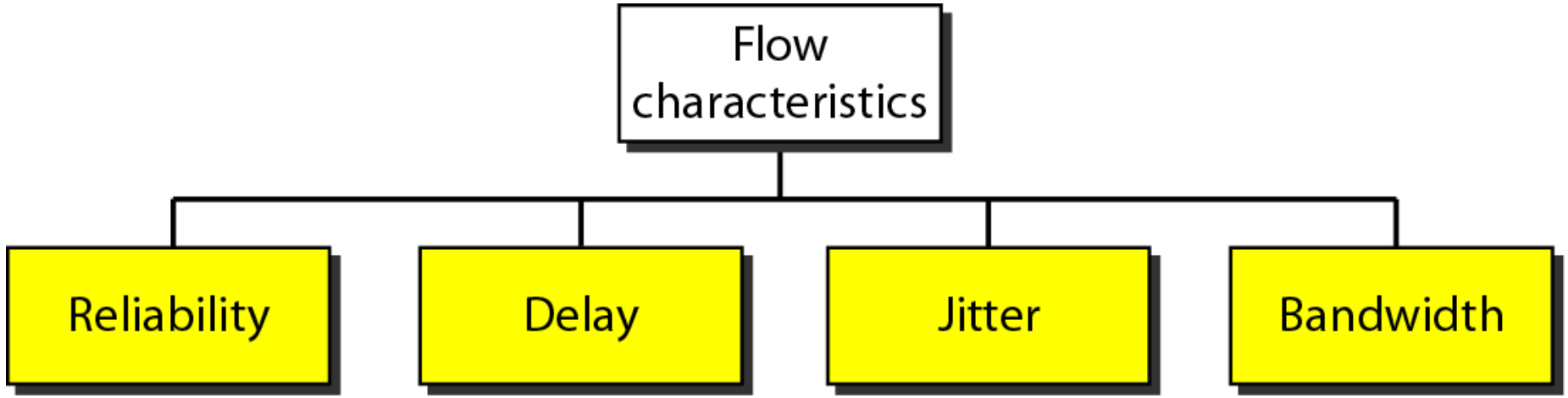
Flow Characteristics

Flow Classes

Quality of Service

- QoS is an overall performance measure of the computer network.
- QoS provides guarantees on the ability of a network to deliver predictable results.
- QoS is a concept used by International Standards Organization (ISO) that specifies how “GOOD” networking services are.
- QoS is especially important for the new generation of Internet Applications such as VOIP, Video- on-demand etc.
- A stream of packets from source to destination is called a flow.

Figure 24.15 *Flow characteristics*



Flow Characteristics

- **Reliability**
- If a packet gets lost or acknowledgement is not received (at sender), the re-transmission of data will be needed. This decreases the reliability. The importance of the reliability can differ according to the application.
- For example: E- mail and file transfer need to have a reliable transmission as compared to that of an audio conferencing.

Flow Characteristics

- **Delay**
- Delay of a message from source to destination is a very important characteristic. However, delay can be tolerated differently by the different applications.
- For example: The time delay cannot be tolerated in audio conferencing (needs a minimum time delay), while the time delay in the e-mail or file transfer has less importance.

Flow Characteristics

- **Jitter**
- The jitter is the variation in the packet delay. If the difference between delays is large, then it is called as high jitter. On the contrary, if the difference between delays is small, it is known as low jitter. Real time audio and video applications cannot tolerate high jitter.
- Example: Case1: If 3 packets are sent at times 0, 1, 2 and received at 10, 11, 12. Here, the delay is same for all packets and it is acceptable for the telephonic conversation. Case2: If 3 packets 0, 1, 2 are sent and received at 31, 34, 39, so the delay is different for all packets. In this case, the time delay is not acceptable for the telephonic conversation.

Flow Characteristics

- **Bandwidth**
- Bandwidth is measured by bits per second. Different applications need the different bandwidth.
- For example: Video conferencing needs more bandwidth in comparison to that of sending an e-mail.
- **Throughput**
- Amount of data transferred from one place to another or processed in a specified amount of time. Data transfer rate for networks are measured in terms of throughput (in terms of Kbps, Mbps).

24-6 TECHNIQUES TO IMPROVE QoS

In Section 24.5 we tried to define QoS in terms of its characteristics. In this section, we discuss some techniques that can be used to improve the quality of service. We briefly discuss four common methods: scheduling, traffic shaping, admission control, and resource reservation.

Topics discussed in this section:

Scheduling
Traffic Shaping
Resource Reservation
Admission Control

Figure 24.16 *FIFO queue*

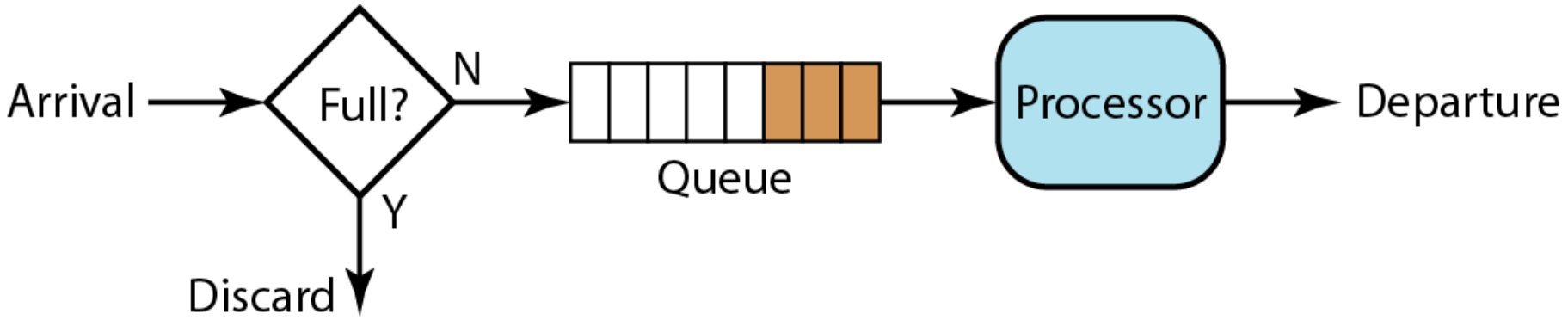


Figure 24.17 *Priority queuing*

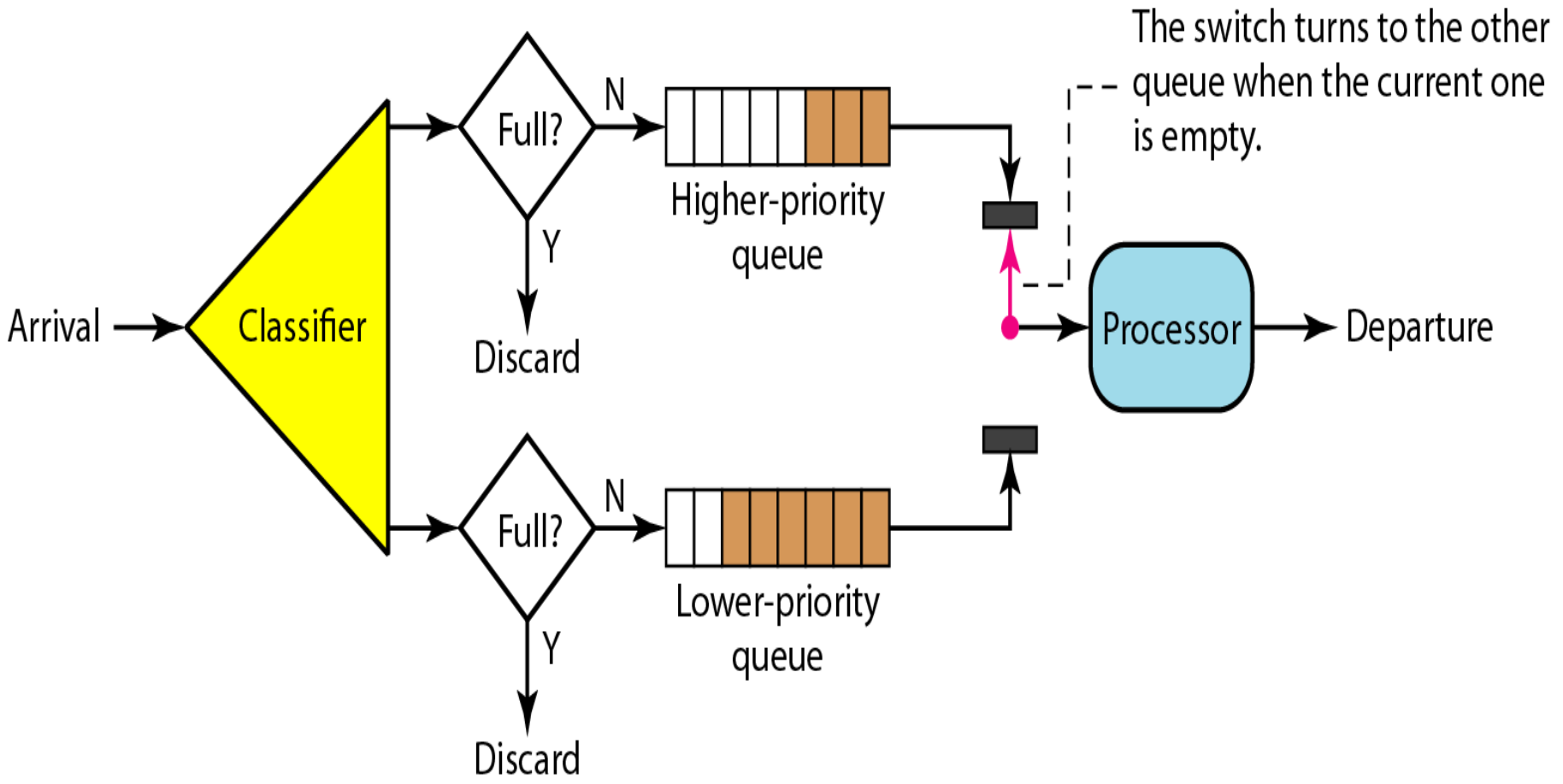


Figure 24.18 *Weighted fair queuing*

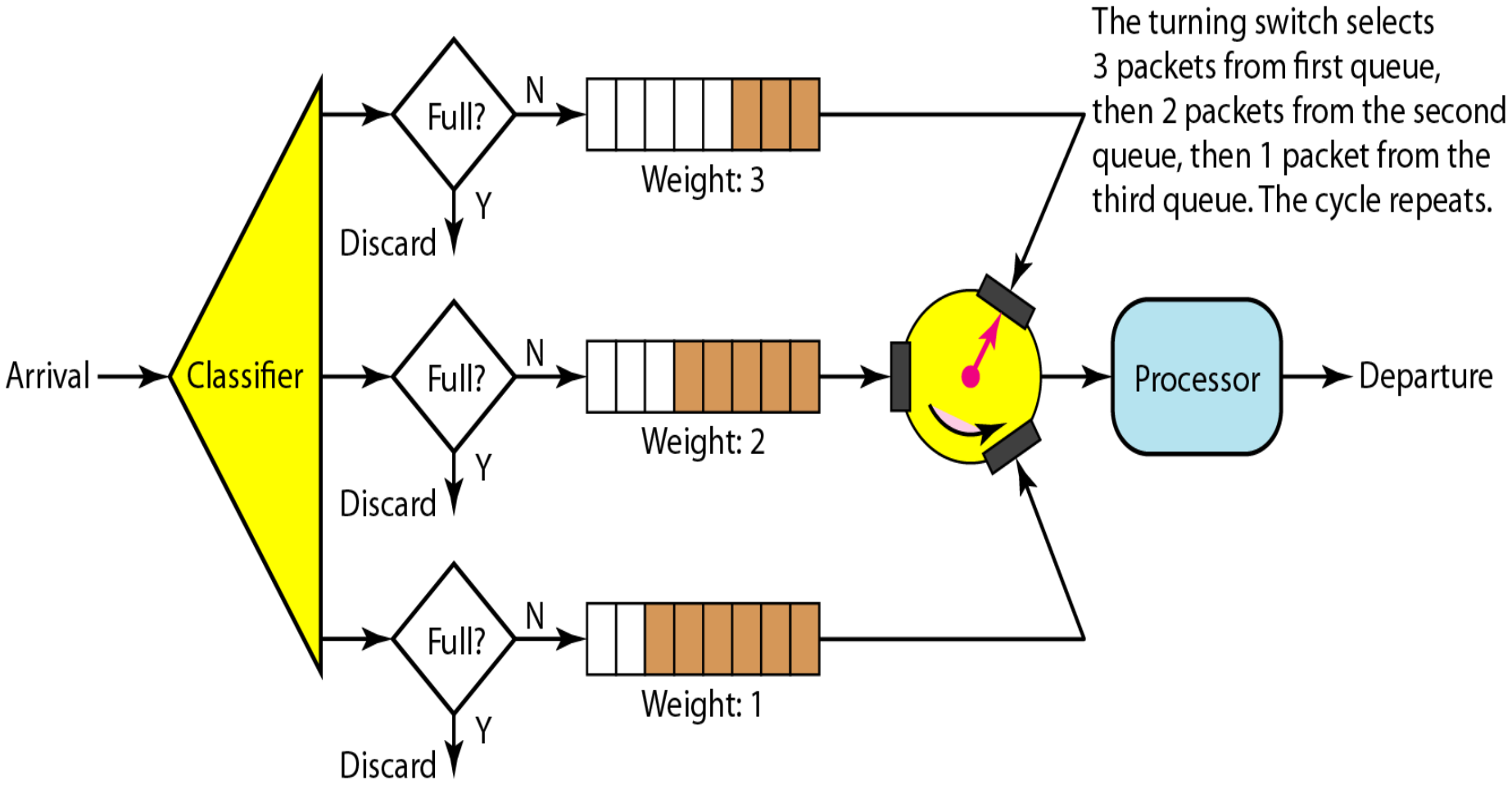


Figure 24.19 *Leaky bucket*

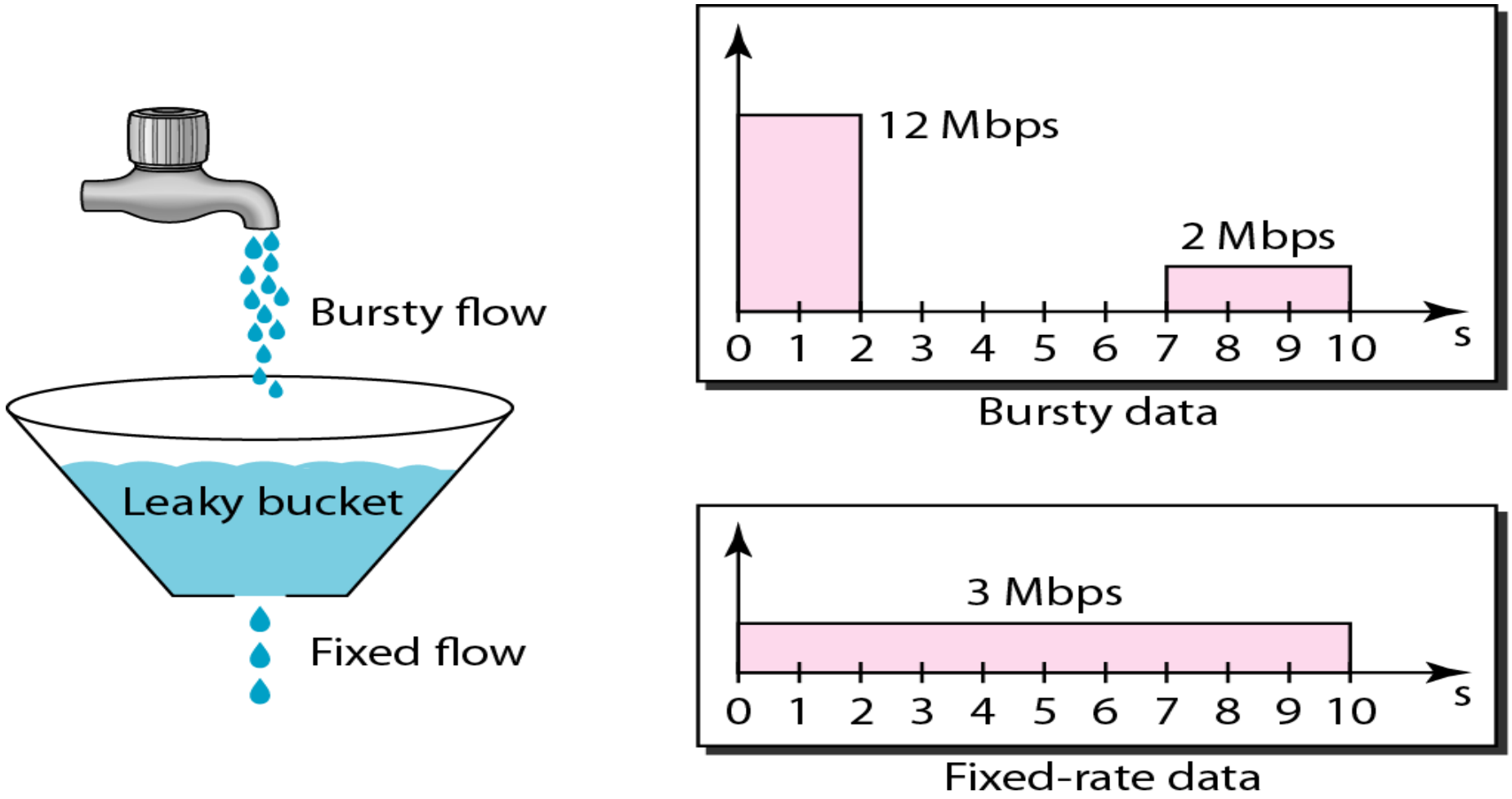
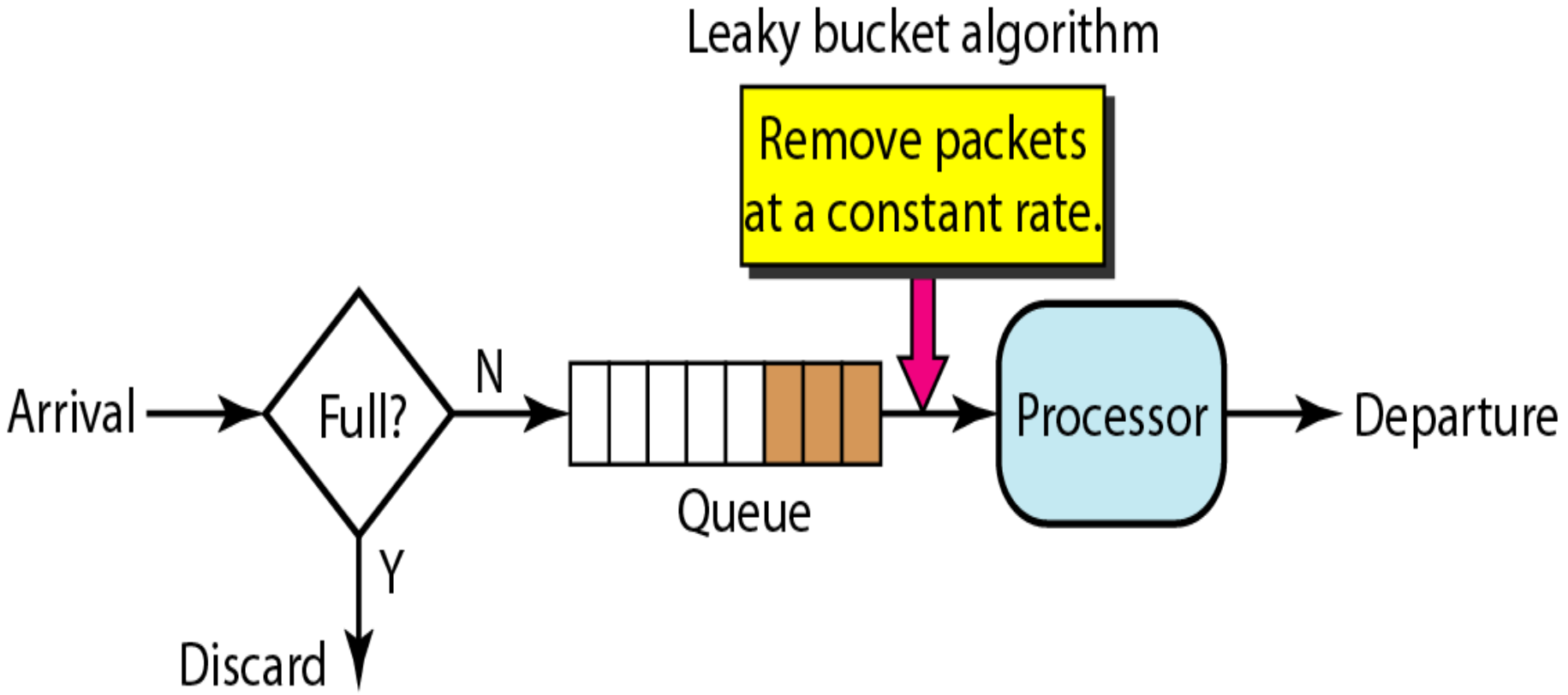


Figure 24.20 *Leaky bucket implementation*



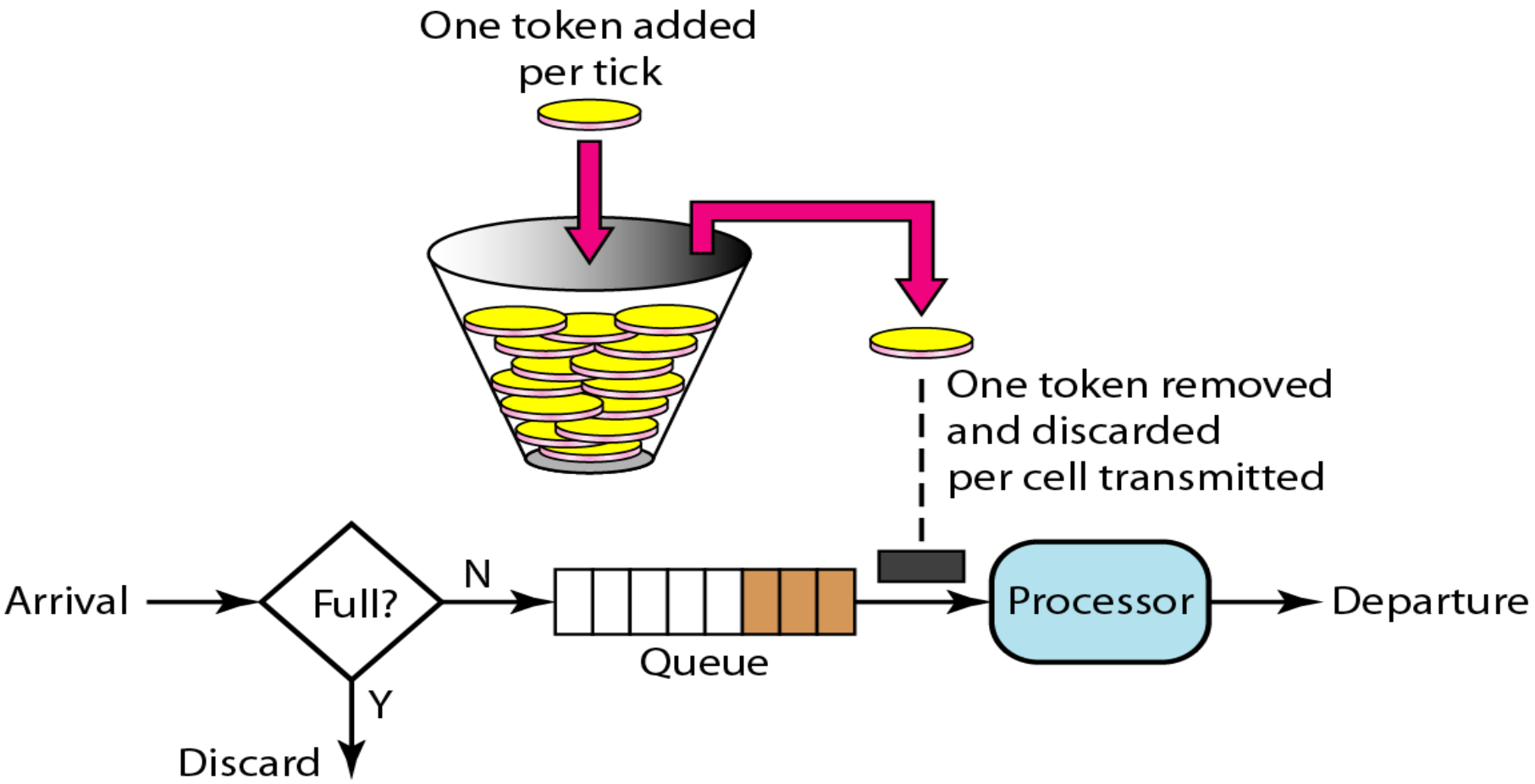
Note

A leaky bucket algorithm shapes bursty traffic into fixed-rate traffic by averaging the data rate. It may drop the packets if the bucket is full.

Note

The token bucket allows bursty traffic at a regulated maximum rate.

Figure 24.21 *Token bucket*



References

- Data communication and networking- Forouzan
- Javatpoint
- geeksforgeeks.org/congestion-control-techniques-in-computer-networks/
- https://www.ques10.com/p/32468/what-are-the-characteristics-of-quality-of-service